Zeus

Operating System

Whitepaper V1.0.5

目录

一、摘　要

当下的区块链行业已经进入了生态应用大爆发的时代，但目前市场上公链生态参差不齐。虽然以太坊最具共识，但其性能堪忧；BSC币安智能链背靠行业巨头流量充沛，但其本质只是一个以太坊的模仿者，无法满足未来日益增长的规模应用；而像SOL、DOT等新型公链却又存在安全及稳定性等诸多问题。因此，我们深刻意识到市场上需要一个真正的应用级底层基础设施，以迎接未来将承载海量应用的元宇宙世界。它必须最大化程度的兼顾公链的"不可能三角"，从而满足未来元宇宙生态的应用需求，构建超级元宇宙生态。

ZOS由此诞生。ZOS全称Zeus Operating System，由美国硅谷ZOS研发团队于2018年6月启动研发，获得众多机构天使轮投资和战略投资。ZOS是全球第一个应用级公链操作系统，以"极轻、极速、极稳"为目标，能够在交易速度快支持海量并发的同时兼顾稳定性，ZOS将构建全球首个满足未来元宇宙生态的底层基础设施，致力于构建超级元宇宙生态。

ZOS 团队首创集群蜂窝式螺旋DAG结构底层系统，深化有向无环结构助力高级节点系统的建立，实现2秒出块，并在此基础上自主研发AI自建无限平行链扩充系统，以承载未来巨大的Dapp生态体系。ZOS通过库协议调用突破智能合约瓶颈，首创独家的超线程技术解决TPS问题，使ZOS公链在最初的版本便可真正突破10万TPS，同时采取智能跨链桥优化跨链解决方案，成功构建了全球第一个应用级公链操作系统。

此外，ZOS公链未来将允许多方式挖矿，支持官方智能挖矿设备、手机矿机（工蜂）、Box终端矿机（验证者）、服务器矿机（守卫者）、超算中心矿机（蜂后）等多维度软硬件集成的蜂窝式系统架构。ZOS基于超前的抗量子理念，为避免未来由量子计算所带来的女巫攻击风险，通过量子超算中心参与节点验证，打造量子级公链安全系统。ZOS未来将通过螺旋迭代，实现ZAI智能学习，ZAI智能代码开源，并建立全球社区自治的激励体系，按照代码贡献率评估机制，奖励ZOS代币用于吸引全球开发者共建ZOS元宇宙开放生态，成为真正的元宇宙基石系统。

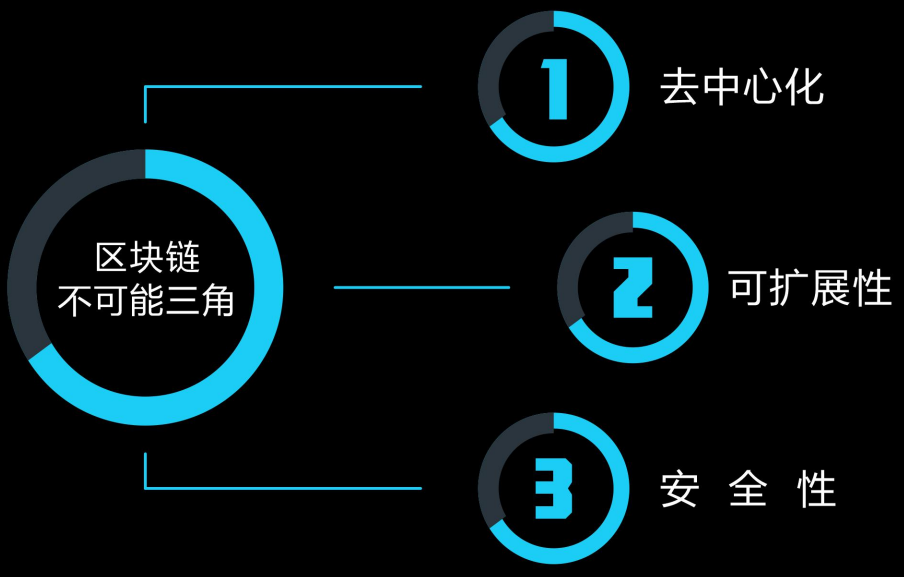
概 述

二、概　述

1.区块链公链现状

1.1 公链的“不可能三角”

稍微对区块链有一些了解的用户应该清楚，区块链技术中有一个“不可能三角”问题，就是去中心化（公平）、效率（可扩展性）和安全性不可能同时做到最优。



一些区块链技术系统更加注重去中心化的公平性，交易效率相对较低；一些区块链技术系统更加注重效率，去中心化的公平性就要被牺牲；强调公平性和效率的同时，也不能忽视安全性。这三者之间的兼顾和均衡，就产生了区块链技术创新的不同方向。

我们深入研究了行业内众多知名公链的底层技术，总结出了它们始终无法完全兼顾的点，每一个公链都有自身无法顾及的方面，从而导致无法满足市场的应用需求，比如未来元宇宙的核心链游应用存在非常多的数据交互场景，那么此时对公链的TPS和稳定性要求极高，如何做到兼顾众多方面使得用户可以只用一条公链就可以满足所有需求，这是一个值得钻研的问题，也是我们的责任。

1.2 公链价值孤岛

区块链行业自2021年以来生态迎来的井喷式发展，但是正因如此也暴漏了行业内最棘手的问题，大量生态应用存在于不同公链之间，导致用户需要来回去各个公链使用不同的应用，非常的繁琐，当今去中心化应用爆发式发展彻底让用户明白了跨链的重要性。

也就是说，目前行业内的基础设施还处于一种孤岛式的割裂状态，各行其道，没能交互联通起来，无法发挥出整体效果。如此条件下，各大公链赛道的竞争，一般而言都是朝着细分领域展开激烈竞争，不太可能同时兼顾像DeFi、NFT、元宇宙链游等众多赛道，所以现在各个赛道应用遍地开花的情况下，跨链的需求就显得尤为紧迫了。

跨链一旦成功，区块链世界的各个赛道就会逐渐被链接起来，形成一张囊括各类通证的区块链价值互联网、代币生态网，发挥整体网络效应，实现价值跨链转移、区块链服务能力互补，降低数字资产流转、交易成本，提升区块链综合服务能力，让大规模商业应用落地成为可能，最终实现区块链蛮荒大陆的大繁荣。

1.3 公链存储问题

对于未来的去中心化应用，尤其是元宇宙领域的应用来说，存储是重中之重，但是目前的公链无法兼顾应用与存储两块，像以太坊这种区块链网络并不是被设计用来存储的，正如大家目前需要用存储都

会去Filecoin和Storj这些去中心化文件存储管理平台一样，市场急需一个可以兼顾去中心化应用的可扩展数据服务。

而这一块目前仍然空白，我们希望能够填补这项需求，并且与其他服务互补，使得整个应用级去中心化底层基础设施更加完整，如果缺少这个部分，去中心化网络将无法有效率地运行和投入像元宇宙生态这种大规模应用。

2、ZOS诞生

2.1 ZOS因需求而生

正如你现在所感受到的一样，元宇宙正在火遍全球，随着Facebook更名为Meta，腾讯、阿里巴巴、百度、网易等各大顶级巨头纷纷表示准备好迎接元宇宙时，毫无疑问，未来将属于元宇宙。

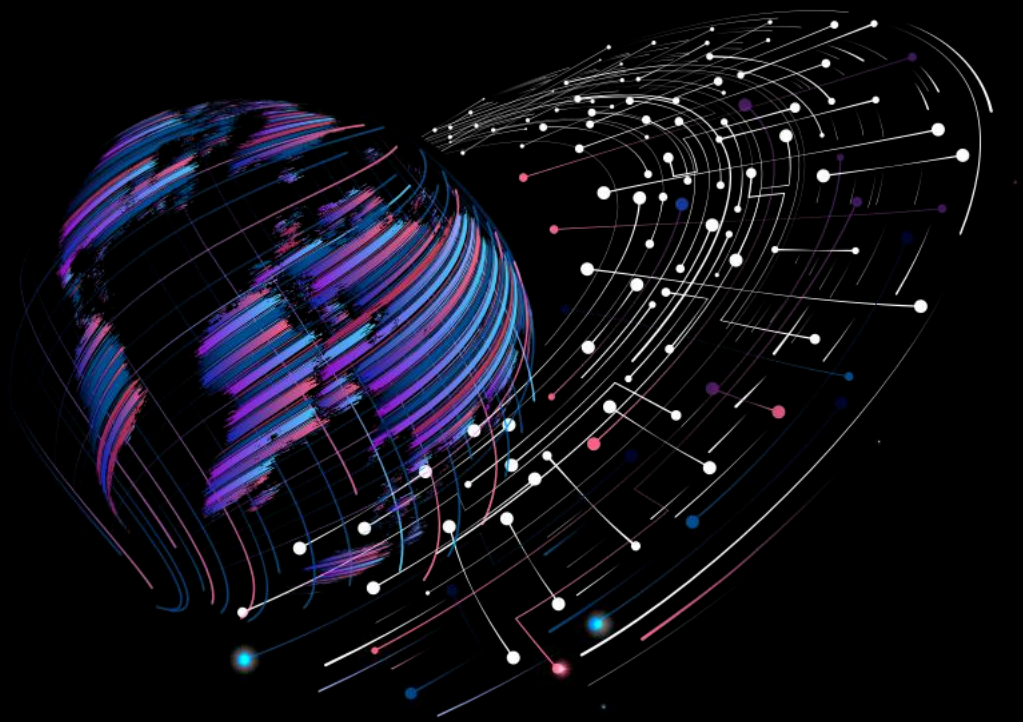
但是正如刚才所分析的那样，元宇宙的底层基础设施并不完善，仍然存在许多问题，根据以上分析得出的种种问题，经过对现有同类项目进行了彻底分析——包括各种知名和有前景的项目分析，总结了每个项目的优势和弱点，我们已经确定了无法找到一个能够各方面都能兼顾的项目能满足元宇宙生态的大规模落地。

譬如以太坊最具共识，用户群体庞大，但其性能堪忧而且手续费较贵，已经沦为了大户专用链；BSC背靠行业巨头流量充沛，但其本质只是一个以太坊的模仿者，无法满足未来日益增长的规模应用；而

像SOL、DOT等新型公链又存在安全及稳定性问题，没有经过庞大的生态应用锤炼。

而目前市场上又急需一个能够兼顾性能、稳定、安全、跨链、存储等多方面的综合性基础设施来参与元宇宙生态，这是我们打造ZOS的理由。

于是我们重鉴于现有项目的局限性，并深入结合了市场需求，优化了公链性能并创新了多项技术和完整的经济模型方案，使得ZOS可以兼顾性能、稳定、安全、跨链、存储等多方面的需求。我们相信，未来ZOS将会凭借强大的实力，可让整个元宇宙生态落地应用得到满足并融入到更为广泛的商业经济中。



关于ZOS

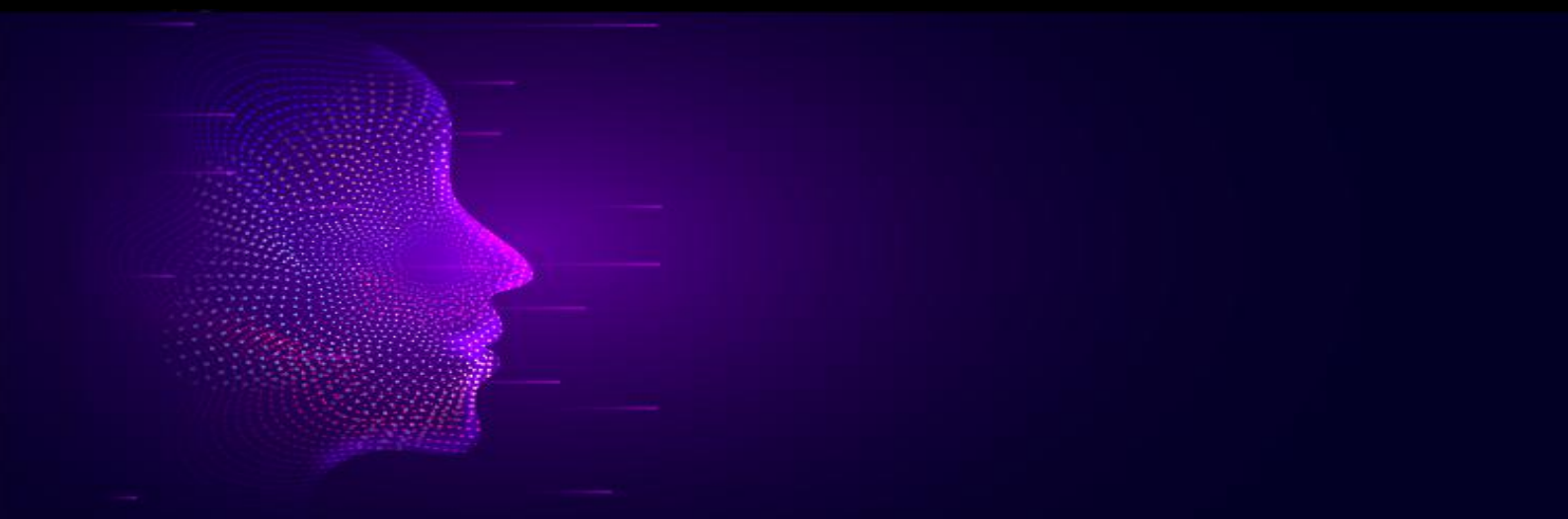
三、关于ZOS

1、ZOS项目概述

1.1 ZOS是什么

ZOS 全称 Zeus Operating System，是全球第一个应用级公链操作系统，以“极轻、极速、极稳”为目标，能够在交易速度快支持海量并发的同时兼顾稳定性，并且支持跨链和存储功能，ZOS将构建全球首个满足未来元宇宙生态的底层基础设施。

ZOS 团队首创集群蜂窝式螺旋结构底层系统，并在此基础上自主研发AI自建无限平行链扩充系统，以承载未来巨大的Dapp生态体系。ZOS公链采用手机矿机（工蜂）、Box终端矿机（验证者）、服务器矿机（守卫者）、超算中心矿机（蜂后）等多维度软硬件集成的蜂窝式系统架构。ZOS基于超前的抗量子理念，为避免未来由量子计算所带来的女巫攻击风险，通过量子超算中心参与节点验证，打造量子级公链安全系统。ZOS未来将建立全球社区自治的激励体系，按照代码贡献率评估机制，奖励ZOS代币用于吸引全球开发者共建ZOS元宇宙开放生态。



2、ZOS团队背景

2.1 ZOS的团队实力

ZOS团队由硅谷知名Team组成，目前已经获得了SBCVC（软银）领投的350万美元种子轮融资，分布式资本、LD Capital、Brightway Future Capital、UpHonest Capital等机构参投。

ZOS将利用这些资金首先把公链基础设施打造完善，形成一个兼顾性能、稳定、安全，同时可以跨链、支持存储的全能型应用级公链。在竞争如此激烈的公链赛道，ZOS为何可以获得资本青睐？因为ZOS团队全员来自硅谷，以斯坦福背景团队为主要班底，囊括了数位法学博士和计算机博士，有斯坦福大学网络与社会中心研究员、旧金山大学数学系与科技法项目主任、国际区块链协会法律顾问、硅谷企业的技术大牛、谷歌工程师和美国上市公司的政府关系负责人。

其核心创始成员在数学、区块链技术、计算机、金融、存储等领域均有十年以上从业经历。团队在学术上的实力尤其耀眼，在斯坦福大学、伯克利大学、牛津大学等出版的顶尖刊物发表了二十多篇学术论文，多篇成果被世界多个权威组织选为推荐读物。

3、ZOS技术亮点

3.1 核心技术创新与应用

3.1.1 创新底层架构

ZOS团队首创螺旋状底层系统软升级模式，深化有向无环结构助力高级节点系统的建立，实现2秒出块，以承载未来海量的元宇宙Dapp生态体系。

3.1.2 三大核心技术

1）库协议调用突破智能合约瓶颈

ZOS实现智能合约编程代码库协议调用，通过把智能合约生成可统一调用的“库”协议，建立高效可编程操作系统，从而极大的提升底层开发相对更复杂大型应用的能力。

2）独家超线程技术解决TPS问题

ZOS独家运用超线程技术(Hyper Threading Technology)，底层主链采用分片技术前提下，在侧链运用超线程实现单个节点多工处理多个程序及TPS的无限叠加可能性，同时提升高并发处理能力。

3）智能跨链桥优化跨链解决方案

ZOS以恒星链底层作为星系中心载体，扩展多个恒星分区用于装载外部公链，引入Z-Smart跨链智能合约与插件协议实现星系链间互通，

通过行星链与卫星链组合结构，实现内外部多链资产交易与Dapp数据跨链交互。

3.1.3 侧链技术

1）原力侧链架构

ZOS 2.0版本上线Force“原力”侧链，采用手机矿机（工蜂）、Box终端矿机（验证者）、aisc矿机（守卫者）、超级节点矿机（蜂后）等多维度软硬件集成的蜂窝式系统架构。

2）存储解决方案

ZOS 支持侧链采用去中心化辰存储方案，通过私钥加密与随机分布式闪电节点的高效传输，为Dapp生态开发者和用户提供金融级别的安全保障。

3）点对点IPv6体系

ZOS 底层多维度软硬件集成架构组成一个覆盖全球的点对点(Point To Point) IPv6体系，由海量终端形成节点群持续贡献存储能力，在传输层有效解决交易网络拥堵问题,在保障安全性的前提下实现性能提升和万物互联。

4）带宽聚合技术

ZOS 研发Z-CDN(带宽加速)技术，让节点提供带宽聚合，提升网络

带宽。

5）抗量子安全性

ZOS 基于超前的抗量子理念，为避免未来由量子计算所带来的女巫攻击风险，将超奇异椭圆曲线同源密码算法应用于节点验证，打造抗量子级公链安全系统。

3.2 ZOS公链特点概述与优势

特点：

- 首创螺旋状底层系统软升级模式，深化有向无环结构助力高级节点系统的建立，实现2秒出块；
- 流水线交易验证机制 ,实现了ZOS站间速率60ms的全新蜂窝式螺旋DAG公有链；

- 支持高并发交易，交易极速确认，测试网最高 TPS 100000+；后续将延拓至百万、千万级别；
- ZOS智能合约库 - Z代码库，满足承载庞大技术逻辑应用需求；
- 交易与合约交互手续费极低，满足所有类型应用；
- 自创哈希算法：Cryptonight & Blake 2b；
- 自创共识协议：ZPOS，完美融合了DAG与POS；
- 自主研发AI无限平行跨链系统；
- 同时兼顾企业级的ZOS文件存储管理服务；
- 超前的抗量子节点验证，防止未来量子女巫攻击；
- 多平台钱包、轻钱包、平行链扩展槽、元宇宙孵化器；
- 全新DAO自治生态激励体系，按照代码贡献率评估机制，奖励ZOS代币用于吸引全球开发者共建ZOS元宇宙开放生态。

优势：

- 可作为虚机的根文件系统
- 可作为元宇宙链游底层设施
- 可承载各类Dapp生态应用
- 可以作为分布式文件数据库
- 可以做雾化Web3.0基础服务
- 支持无限平行跨链

ZOS

技术详解

四、ZOS技术详解

1、公链底层技术DAG详解

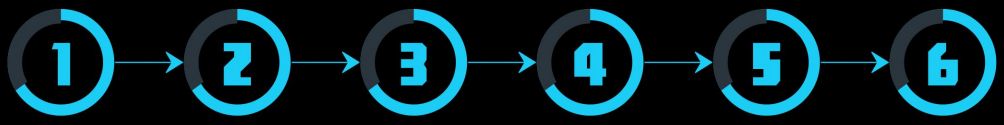
1.1 公链协议 - 有向无环图（DAG）

ZOS 团队首创螺旋结构底层系统软升级模式，并在此基础上自主研发Z-Ai智能自建无限平行链扩充系统，深化有向无环结构助力高级节点系统的建立，实现2秒出块，以承载未来巨大的Dapp生态体系。

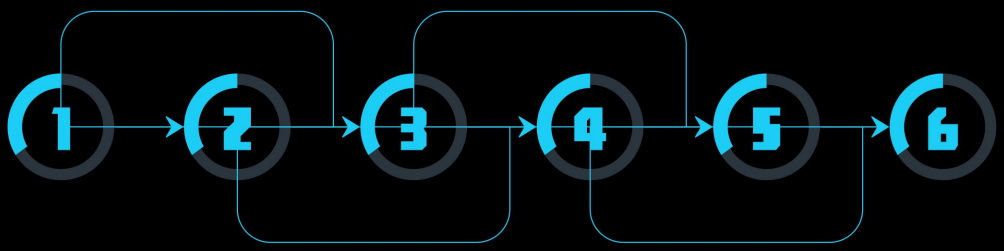
在开始讲解之前，我们首先需要为大家呈现出ZOS的整体技术架构：

首先我们将会从ZOS的公链协议层讲起，因为ZOS团队意识到，如果想满足更大规模的应用落地，实现超高的TPS满足元宇宙生态需求，就必须使用DAG结构来改进公链底层协议。

若一个有向图无法从某顶点出发经过若干条边回到该点，则称该图为有向无环图（Directed Acyclic Graph，DAG）。使用 DAG 数据结构存储区块链账本数据的模式，正逐步受到更多开发者的关注。我们希望可以使用蜂窝式螺旋 DAG 结构构建能够长期稳定运行的公有链，来证明 DAG 链的技术先进性和性能。



[传统区块链]



[D A G]

在ZOS中，交易被视为一种消息，支持多种类型的消息，多个消息可组合成一个数据块，该数据块称为一个单元（Unit），单元与单元之间相互链接组合成一个 DAG 图。由于单元可以链接到任意一个或多个之前的单元，不需要为共识问题付出更多的计算成本和时间成本，也不必等待节点之间数据强同步，甚至没有多个数据单元拼装

区块的概念，因此可以极大提高交易的并发量，并把确认时间降低到最小。

ZOS使用以下方案解决双花问题。首先，尝试在 DAG 图上找到一条以创世单元为起点的主链，并给位于主链上的单元分配索引，创世单元索引为0，创世单元的子单元索引为1，以此类推。然后，对于不在主链上的单元，定义其索引等于引用此单元的第一个主链单元的索引。最终，DAG上的每笔交易都拥有了一个索引。如果两笔交易尝试使用同一笔输出，只需要比较其索引的大小，小的有效，大的无效，由此解决双花问题。

始于对现有加密货币局限性的探讨，也是整个ZOS项目的基础。ZOS的愿景是提供一个便捷、安全、可扩展、以用户为中心的区块链，以及可被广泛采用的加密货币生态系统。结合ZPOS协议和Black2b哈希算法，我们提出了一种既安全又方便的新型DAG公链。通过采用本白皮书所阐述的办法，ZOS加密货币为全球加密货币环境提供了一种有价值的、差异化的补充。

1.2 数据结构

在ZOS网络中，当节点发起交易或发送消息时，首先创建一个新的数据块并广播给 peer 节点，称为“单元（Unit）”。一个单元可以包含多个不同类型的消息，单元中包含以下内容：

头部：当前单元所引用的之前单元（父单元）的哈希值。

消息组：一个单元可以包含多个消息（Message），消息有多种不同类型，每种消息都有自己的数据结构定义。

签名：对所创建单元的一个或多个用户的数字签名，单个用户可以拥有多个地址，地址利用 BIP-0044 算法生成。

1.3 改进账本结构 - Zone结构

ZOS发现账本结构的改进方向是构造等价类，基于此可以实现自动螺旋式升级+火箭脱落式去冗余，ZOS将多个交易全局有序的线性账本规约为一个只记录部分偏序关系的非线性账本，这种非线性账本结构是一个DAG，可以支持高阶智能合约声明，而且未来可以对账本结构进行迭代升级，类似于IOS操作系统1.0、2.0、3.0.....

1.4 改进系统状态

ZOS对系统状态的主要改进思路是将全局的世界状态局部化，每个节点不再关心全部交易和状态转移，只维护整个状态机的一个子集。这样集合S和集合T的势都大为缩减，从而提高了系统扩展性，方便实现跨链，此系统参考了包括：Cosmos，Aelf等项目。

1.5 改进哈希算法 - 量子超算

早期ZOS对系统状态采用Blake2b作为系统中唯一的哈希函数，而随着 ASIC技术的最新发展，Blake2b逐渐被抗矿机

（ASIC-resistant）的 Cryptonight算法所取代。Cryptonight算法工作时使用伪随机内存读写操作，故与标准ASIC体系结构不兼容，却使得CPU与GPU的工作性能差别相对不那么明显 ,这样可以实现自研芯片与矿机。

今后，为了防止采掘资源的中央化，我们计划实现手机矿机、Box终端矿机、服务器矿机、超级中心矿机等多维度软硬件集成的蜂窝式系统架构，并定期调整哈希算法，以在开采期间维持ASIC阻力，同时也能够防护量子计算机的攻击。

2、ZOS智能合约库：Z-代码库

2.1 Z代码库 - 强大的多维Dapp底层代码通用组件

ZOS技术生态中专门制作了一套SDK，用于ZOS生态开发者设计的开发组件，这是ZOS DAG框架中不可或缺的一部分。ZOS SDK融合了以太坊开发语言，兼容Solidity，开发者可以通过ZOS SDK轻松构建区块链和去中心化应用（DApps）。

ZOS实现智能合约编程代码库协议调用，通过把智能合约生成可统一调用的"库"协议，建立高效可编程操作系统，从而极大的提升底层开发相对更复杂大型应用的能力。

我们都清楚，目前的所有公链，智能合约开发是有字节长度限制的，代码重叠效率低，所以只能做一些小型Dapp应用程序。

而ZOS启用了Z-代码库，可以实现开发更复杂的应用程序，为元宇宙提供强大应用。ZOS将合约层代码存入N个标准“库”中进行集中编译调取，提升了智能合约字节数量，简化繁琐臃肿的开发语言代码，降低开发门槛，使智能合约简易的瓶颈得到突破，实现复杂的大型应用开发。

未来的元宇宙生态落地一定是伴随着庞大的运行代码体系，目前的公链无法适应其后期需求，所以我们提前看到了这一点，并于现在就已经着手于落实Z-代码库，以实现未来元宇宙生态的完美落地应用。

3、ZPOS共识机制细节

3.1 ZPOS机制详解

ZPOS是我们选择的PoS协议，相较于传统POS机制，ZPOS实际上是结合了DAG模块的POS版权益证明机制，不仅效率更高，而且可以有效防止恶意分叉。

这里我们可以使用传统“罗马议会”运行的机制来解释它。

传统的区块链好比“罗马议会”每几秒或者10分钟选择一个“本届议长”，但是每一届的议长都很懒，每一个任期只能处理几十或者上百个公务，剩下的时候就在睡觉。其他公务就只能排队。谁出的钱多（矿工费）就优先处理谁的公务。显然在这个“共识模型”中，整个罗马帝国的效率瓶颈都集中在了这个“议长”的处理效率中。

而ZPOS呢，首先“罗马议会”先建造一个“罗马神庙”（共识智能合约），然后再选出各个地方的“议员”，然后在各个议员选一个当“本届议长”。只要持币超过一定数量的ZOS就可以成为“议员”的候选人。选完立刻记录在“罗马神庙”中，只要个人财富排在30名（每轮出块列表中持币ZOS量在30名以内）的议员就可以成为真正的“议长候选人”，议长候选人之间互相投票（根据类DAG算法进行块引用），其中“能力最强”的候选人则成为本届议长（随机数算哈希最小的），任期只有15秒左右，每届议长的权力有限且只能根据“罗马神庙的契约”跟民众收税（PoS出块奖励）。

其中选议员的过程就是PoS过程（按持币量），选议长的过程就是PoW过程（按PoW算力），此时PoS/PoW完美的结合在一起。

为了防止有人恶意去使得我们的区块链产生分叉，那么我们想方设法去对恶意制造者加以惩罚，这样就可以解决无成本利益关系问题。

首先，在ZPOS中，验证者押下一定比例的他们拥有的ZOS作为保证金。

然后，他们将开始验证区块。也就是说，当他们发现一个可以他们认为可以被加到链上的区块的时候，他们将以通过押下赌注来验证它。

如果该区块被加到链上，然后验证者们将得到一个跟他们的赌注成比例的奖励。

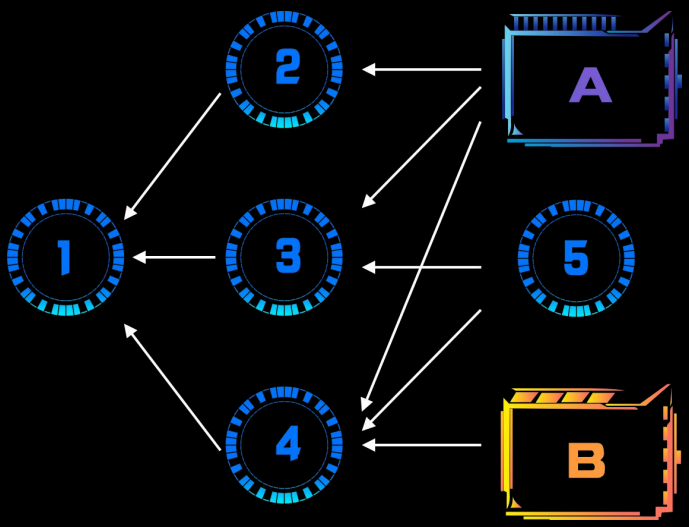
但是，如果一个验证者采用一种恶意的方式行动、试图做"无利害关系"的事，他们将立即遭到惩罚，他们所有的权益都会被砍掉。

正是利用了这样的对赌协议，帮我们对恶意制造者加以了惩罚，使得我们的区块链尽量保障不会产生分叉。

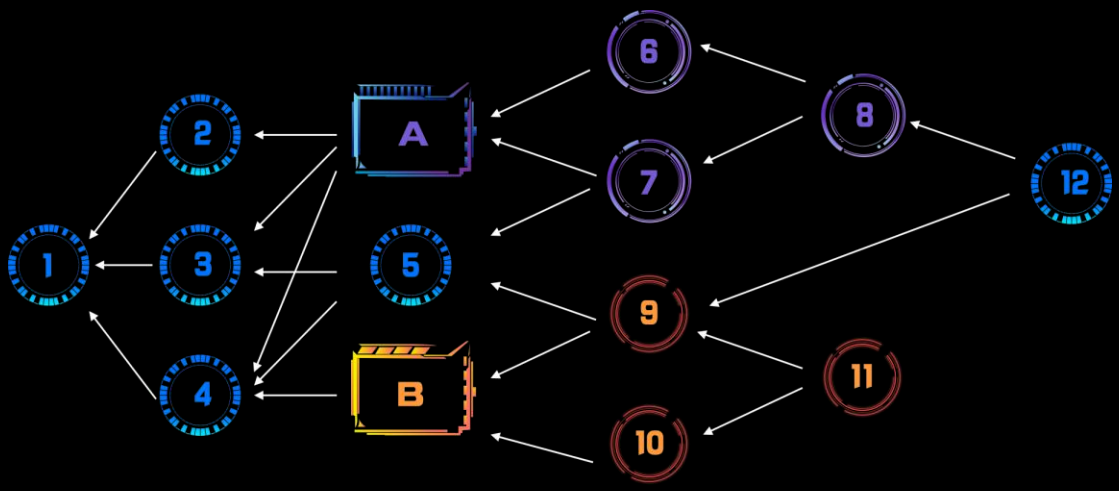
3.2 ZPOS双重支付举例

还是通过举例的方式，块A包含交易t1，块B包含与之冲突的交易t2，这些冲突可能是恶意的，也可能仅仅是由于节点间的延迟导致了交易被发布了两次，这样两个矿工就会收取相同的交易费。根据DAG结构的不同，块A和块B可能拥有不同的先行块和后续块，双重支付的解决方式也不尽相同。

这个例子的初始情况可能如下所示：块A和块B几乎与块5同时添加进来。

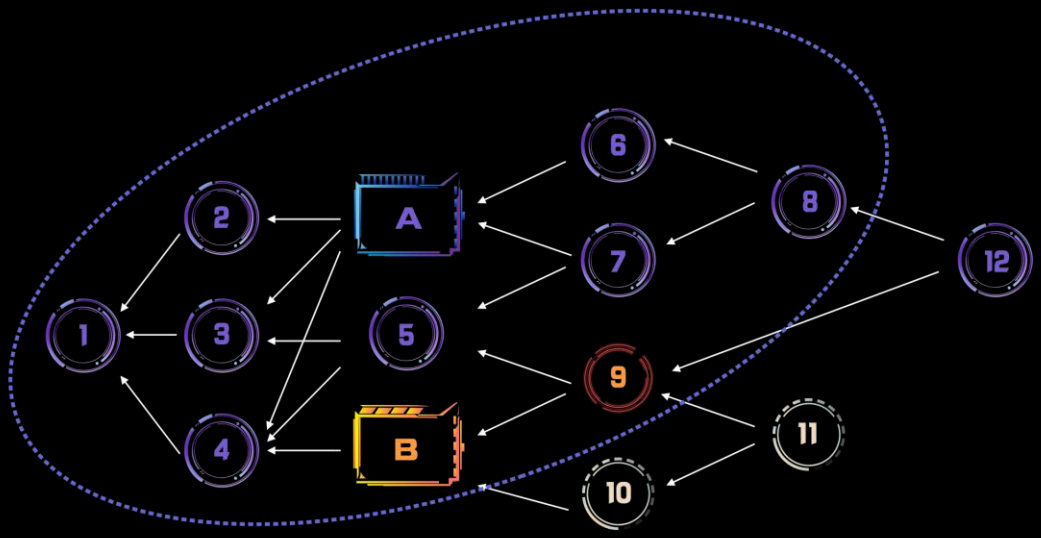


系统在这个阶段并没有意识到双重支付，因为互为冲突的块A和块B之后尚没有新块产出。但是随着DAG的发展，更多的块添加进来，双重支付的问题浮现，这时就需要分析整个DAG结构来决定块A和块B之间哪一个是先行块。



在上面的图中，块12是第一个把块A和块B作为先行块的区块，从而检查到双重支付。根据前面介绍的投票规则，块6、7、8都投票给块A，因为块B不是他们的先行块。同样的道理，块9、10、11都投票给块B。

块12的投票是基于对其先行块的递归投票查询。因为块10和块11不是块12的先行块，故它们不包括在块12投票时的查询范围。块12投票时参考的查询范围如下图所示。



其中块1到块5不属于块A和块B的后续块，所以它们的投票结果取决于它们大部分的后续块。在这个递归投票的例子里，块1到块5的后续块更多的会投票给块A，故它们也投票给块A。块12的先行块里有9票投给块A，2票投给块B，所以块12会投票给块A。如果投票数相同，将由块12投出决定性的一票，故所有参与者都赞同块12的投票方式。由于块12只使用它的先行块（past(12)）来决定选票，所以它的投票永远不变。

DAG结构中接下来的投票是基于其他块的后续块。一旦块12的投票结果确认了，块5也会投给块A，因为后续块中有三票投给了块A(块7、8和12），多于块B的两票（块9和块11）。块4的后续块中，块A、5、6、7、8和12投给了块A，块B、9、10和11投给了块B，所以块4也投给块A。同理，块3、2、和1也都会投票给块A。所以，这

个投票过程的最终投票统计为，块A得10票，块B得4票。

ZPOS一个有趣的特性是 ,它符合了其他区块链技术中采用的最长链选择模型，特别是在像上面演示的这样简单的例子里。可以看出，从块1经由块A到块12的路径，要比经由块B到块12的路径长，即最长的链路获胜。

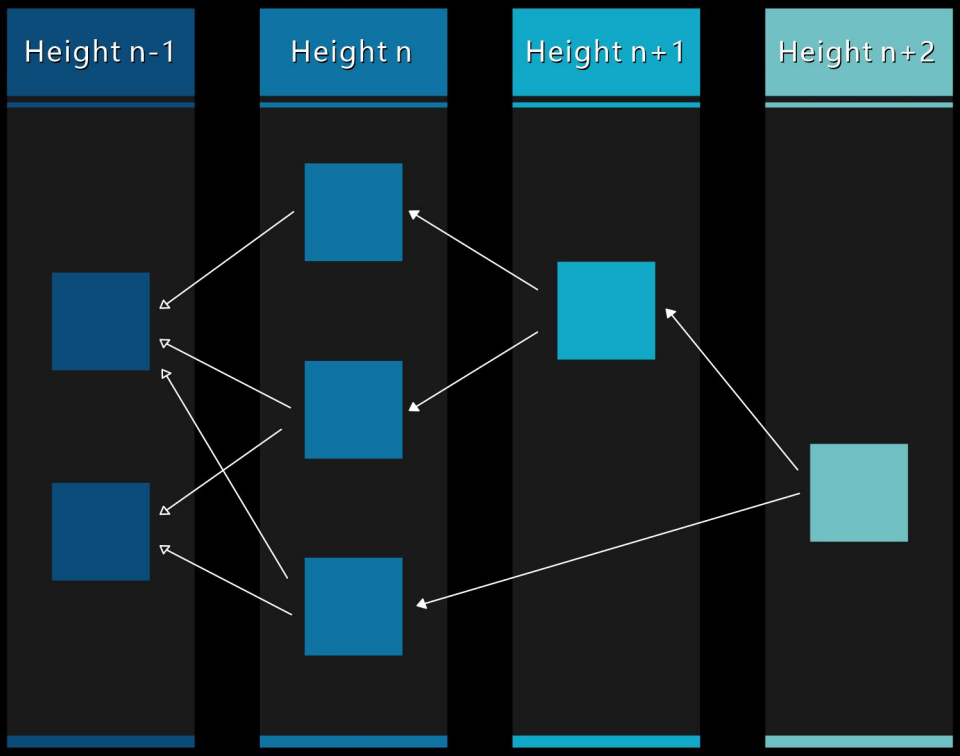
3.3 块的高度和链接

粗略地看一下DAG结构 ，可以看出用在比特币或以太坊中的区块高度的传统概念需要进行细微的语义上的修改。在那些具有代表性的区块链中，高度代表了链接在创世区块上的块数。而在ZOS中，高度是一个更加笼统的描述，表示当前块在创世区块之上的DAG层数。其中的计算非常简单，新块的高度比它最高的父块的高度要高一层，根据我们的计算，大约每秒出一个块。

对于任一新块 B，与其父块 P：

Height（B）= max（Height（p））+1；p ∈ P

用图表表示就如同下面提供的示例，新发布的块关联到最高的未被关联的块上，并将高度设置为比最高的关联块多一



4、ZOS 流水线交易验证

4.1 流水线验证交易机制

ZOS为了可以让自身拥有超高性能满足元宇宙生态落地，拥有超过10W+TPS以及亚秒级的交易能力，我们研发了一种快速验证大量交易块的方法，我们称之为流水线验证机制。

为了实现它，我们参考了CPU设计中的常见流水线机制，当有一个输入数据流需要通过一系列的步骤来处理，并且有不同的硬件负责每一个步骤时，流水线便是一个极为合适的优化方案。解释这一现象最典型的比喻是一个洗衣机和烘干机，它们依次清洗/烘干/折叠几件衣服。洗涤必须发生在干燥之前，干燥必须发生在折叠之前，但这三

项操作中的每一项都是由一个单独的单元来完成的。

为了最大限度地提高效率，ZOS创建了一个阶段性的流水线。我们可以称洗衣机为第一步，烘干机为第二步，折叠为第三步。为了运行这个流水线，在第一件衣服被放到烘干机之后，就会将第二件衣服放到洗衣机中。同样，在第二件衣服放入烘干机，第一件衣服被折叠之后，再将第三件衣服放入洗衣机。通过这种方式，人们可以同时洗三件衣服。考虑到无限负载，流水线将始终以流水线中最慢阶段的速度完成负载。

ZOS在软件中创建了一个四阶段交易处理器，称为TPU，即交易处理单元。

在ZOS网络上，流水线机制（交易处理单元）通过内核级的数据获取、GPU级的签名验证、CPU级的银行和在内核空间的写入来进行。当TPU开始向验证器发送区块时，它已经获取了下一组数据包，验证了它们的签名，并开始计入代币。

验证器节点同时运行两个流水线进程，一个用于领导者模式（TPU），一个用于验证器模式（TVU）。在这两种情况下，流水线化的硬件是相同的，包括网络输入、GPU卡、CPU内核、写到磁盘和网络输出。TPU的存在是为了创建分类账条目，而TVU的存在是为了验证它们。

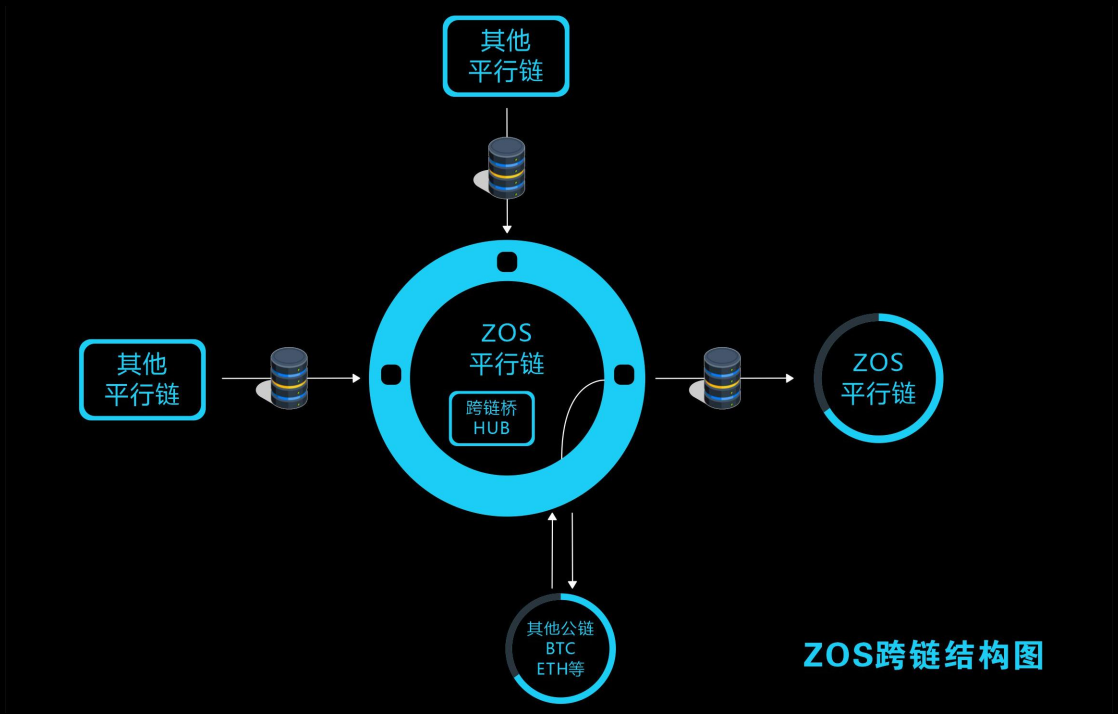
在这个四阶段流水线的GPU并行化过程中，在任何特定的时刻，ZOS TPU可以同时处理超过100000笔交易（测试网测试成功）。

总结来看，我们找到了一个方法，参考了CPU的设计机制，可以让所有硬件一直保持忙碌状态，最终实现了性能的提升。

5、ZOS 跨链解决方案

5.1 ZONE异构跨链结构

我们可以看到 ,随着市场上应用火热起来 ,无论是侧链还是Layer2等扩展方案都纷纷崭露头角 ,而想要完全满足于目前市场应用就必须要让ZOS支持完备的跨链方案，我们为ZOS设计了拥有COSMOS的HUB底层与ZONE结构予以实现。



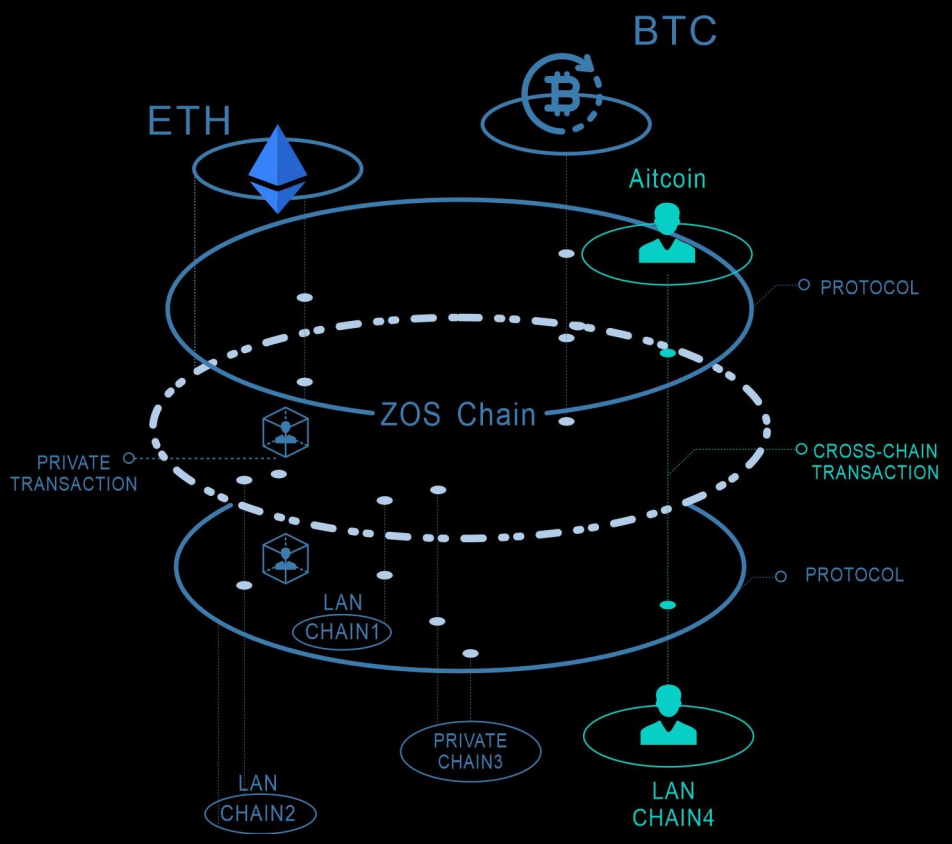
ZOS跨链结构图

5.2 ZOS中继桥HUB

ZOS Hub中心是一种多资产权益证明网络，它通过简单的管理机制来实现网络的改动与更新，还可以通过连接其他空间来实现扩展。

ZOS对于跨链交易，会利用多方计算和门限密钥共享方案。当一种未注册资产由原有链转移到ZOS链上时，ZOS链节点会使用一个基于协议的内置资产模板，根据跨链交易信息部署新的智能合约创建新的资产。当一种已注册资产由原有链转移到ZOS链上时，ZOS链节点会为用户在已有合约中发放相应等值代币,确保了原有链资产在ZOS链上仍然可以相互交易流通。

ZOS HUB网络的中心及各个空间可以通过区块链间通信（IBC）协议进行沟通，这种协议是针对区块链网络的，类似UDP或TCP网络协议。代币可以安全快速地从一个空间传递到另一个空间，两者之间无需体现汇兑流动性。相反，空间内部所有代币的转移都会通过ZOS HUB中心，它会记录每个空间所持有的代币总量。这个中心会将每个空间与其他故障空间隔离开。因为每个人都可以将新空间连接到ZOS HUB中心，所以ZOS HUB也可以兼容未来新的区块链，正如下图：



ZOS以恒星链底层作为星系中心载体，扩展多个恒星分区用于装载外部公链，引入Z-Smart跨链智能合约与插件协议实现星系链间互通，通过行星链与卫星链组合结构，实现内外部多链资产交易与Dapp数据跨链交互。

6、ZOS分布式存储

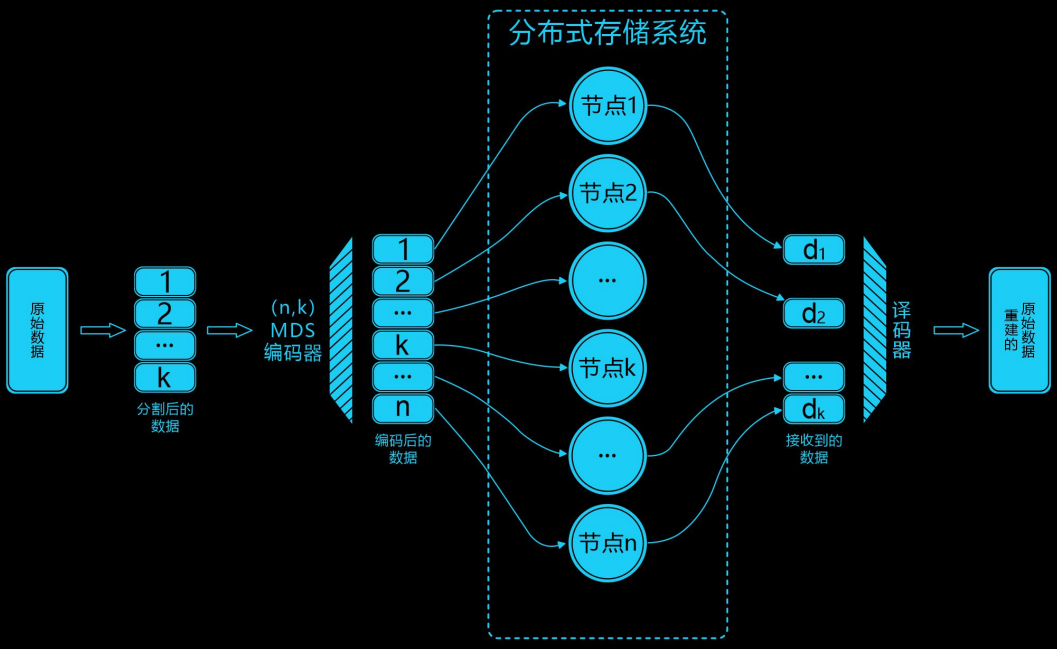
6.1 存储解决方案

ZOS支持侧链采用去中心化辰存储方案，通过私钥加密与随机分布式闪电节点的高效传输，为Dapp生态开发者和用户提供金融级别的安全保障。

6.2 独创的雨存储系统

ZOS在分布式存储技术方面基于IPFS的技术进行研发创新，在DAG链的基础上用分布式哈希表这种数据结构被用来执行文件的分发工作，实现了高协调性的ZOS雨存储系统。该系统的搭建可以有效地协调，实现节点之间的有效访问和查找。通过分布式哈希表，节点可以存储和共享数据，而无需中央协调。

ZOS利用DAG确保在p2p网络上交换的数据块是正确的、没有受到损害的和未被修改的。在ZOS 雨存储中，哈希值替代了传统互联网体系中的URL，利用独一无二的哈希值，能够轻易验证存储于ZOS网络中信息的真伪及完整性（ZOS上的所有内容能够被唯一地标识，因为每个数据块有独一无二的哈希值。此外，数据是防篡改的，因为数据的更改会改变哈希值）。



7、ZOS 云计算协议

7.1 点对点IPv6体系

ZOS 底层多维度软硬件集成架构组成一个覆盖全球的点对点(Point To Point) IPv6体系，由海量终端形成节点群持续贡献存储能力，在传输层有效解决交易网络拥堵问题，在保障安全性的前提下实现性能提升和万物互联。

7.2 Z-CDN加速协议

ZOS的DAG核心网络一方面作为区块链，提供公开不可篡改的记账能力；另一方面会作为 AI 数据平台，动态感知用户需求及网络状态的变化，进行全局资源调度，满足全网体验最优，使成本变低。

ZOS已申报IPv6资源，使得ZCDN产品可以完全满足IPv6的应用需求，避免了常见的延时、成功率低以及稳定性不足的问题。另外，ZOS的存储网络聚合存储矿工的存储能力，提供近乎无限的存储空间，信道编码[1,16]进一步降低冗余备份数量，存储可靠性提高到99.99999%。存储网络以冷数据为主。加速网络聚合过剩闲置资源的带宽能力，提供 100Mbps 的超高速传输服务，加速矿工最小剩余存储空间只需 50MB；由 AI 算法基于全网状态完成缓存数据在全网加速矿工的调度。加速网络以热数据为主。

总的来说，ZOS研发的Z-CDN(带宽加速)技术，让节点提供带宽聚合，提升网络带宽。

7.3 ZOS边缘计算

ZOS考虑到未来物联网的应用落地，将ZOS与物联网中边缘计算结合，现在ZOS的边缘计算已经解决了安全、计算资源分配不均等诸多问题。

传统的物联网领域，都是基于服务器的中心化结构，所有设备的链接、数据处理都需要经过云计算，现在已经暴露出，诸如计算成本高、数据保护没法监管、被攻击后造成连锁反应的问题。现在ZOS通过独创的加边缘计算技术和DAG优势去解决它。在靠近物联设备终端的位置上，进行数据处理，即设备在原先可以交互，并产生数据的情况下，现在能做到自行处理计算数据，通过局部数据计算，就可以实现物联设备的智能控制。

8、抗量子安全系统

衡量密码方案安全性的指标是安全等级，安全等级的具体参数通常可由系统的参数大小计算(这里没有考虑公钥密码方案的安全性证明中攻击者攻破系统的优势与解决方案基于的困难问题的优势之间的归约损失，换句话说，我们这里简单地认为方案地安全等级由系统的参数大小计算）。可以参照很多国际标准（nist、fips等）。常用

的模乘群（Zp*），有个问题在于存在比一般性算法时间复杂度更低的亚指数级解决离散对数问题的算法，因此模数p的二进制长度要加大以保证安全性。比如，80bit安全需要1024bit的p。

椭圆曲线的引入则针对上述问题，进行优化。目前已知的最优的解决（安全的）椭圆曲线上定义的群下离散对数问题的算法，时间复杂度是指数级（即一般性算法，复杂度为群的阶（假设为素数阶）的平方根）。因此为了达到80bit安全，仅需群的阶达到2^160即可。根据Hasse定理，椭圆曲线群的阶与定义的有限域Fp中的模数p大致相等。即定义椭圆曲线的模数p大致取160bit即可达到80bit安全性。相较于模乘群的1024bit规模，虽然椭圆曲线群的操作更复杂，但效率更高（因为计算在更小规模的模数下）。 而椭圆曲线可以分为超奇异椭圆曲线和一般曲线。超奇异曲线的定义有多种等价形式，举较容易理解的一例说明：曲线E定义在有限域F_{p^r}下（可以取r=1，即素域Fp），椭圆曲线群的阶#E(Fp)满足#E(Fp)=1 mod p，则称曲线为超奇异曲线。

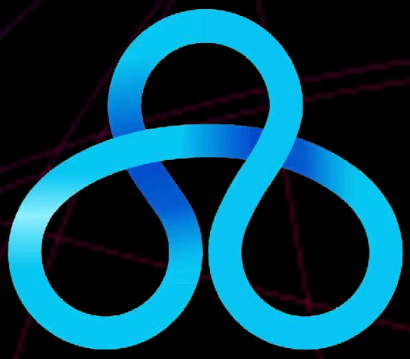
由于椭圆曲线群下离散对数问题更困难，模乘群（有限域）下的存在亚指数级算法。那么有学者就提出是否可以把椭圆曲线群下的问题转化为有限域下，从而更快求解。MOV攻击和FR攻击就是基于这种思想提出的，借助的就是双线性对工具，就是图片上的定义。weil对或者tate对都是具体构造双线性对的方法，细节需要进一步参考相关书籍。例如给了椭圆曲线下的离散对数问题(P, kP)求k，我们计算e(P, P)和e(P, kP)=e(P, P)^k，相当于得到了一个有限域下的离散对

数问题(e(P, P), e(P, P)^k)求k。攻击者就可以选择这两个里面较容易地一个问题去求解。双线性对将两个椭圆曲线群上的元素映射为一个有限域下的元素，这个有限域是定义椭圆曲线的域Fp的一个扩域F_{p^k}。具体的k的值可由满足等式p^d=a mod N的最小正整数k计算（N是#E(Fp)的一个素因子）。参照国际标准推荐的系统参数大小，p（参考椭圆曲线群）和p^k（参考有限域/模乘群）哪个更容易，方案的安全性就取决于更低的那个（木桶原理）。

椭圆曲线的优势在于离散对数问题更难，但如果存在双线性对这种转化那是有隐患的。因此希望k的值大些好，使得p^k对应的有限域下问题求解难度远大于p对应的椭圆曲线下的问题。针对绝大多数曲线而言，这不是问题，因为有证明大多曲线（随机选取）的k值跟N（大素因子）的规模相当。因此，问题就出在那些不一般的曲线上。MOV攻击证明了，对于超奇异椭圆曲线，k值小于等于6。所以，这类曲线如果参数选取不好（恰巧k值较小），就面安全隐患。

事情都具有两面性，实际上，双线性更多的应用是用来构造密码方案。因此只要参数选取得当，可以带来更多的正面应用。如果随机选取曲线，根据之前的结论，k值与N相当，那么根本无法计算双线性对。为了使用双线性对工具，则需要合适的参数确定合适的k值。这时，超奇异椭圆曲线就是一个选择。

ZOS系统便是基于超前的抗量子理念，将超奇异椭圆曲线同源密码算法应用于节点验证，以避免未来由量子计算所带来的女巫攻击风险，打造抗量子级公链安全系统。



ZOS

价值体系

五、ZOS价值体系

1、ZOS原生资产代币

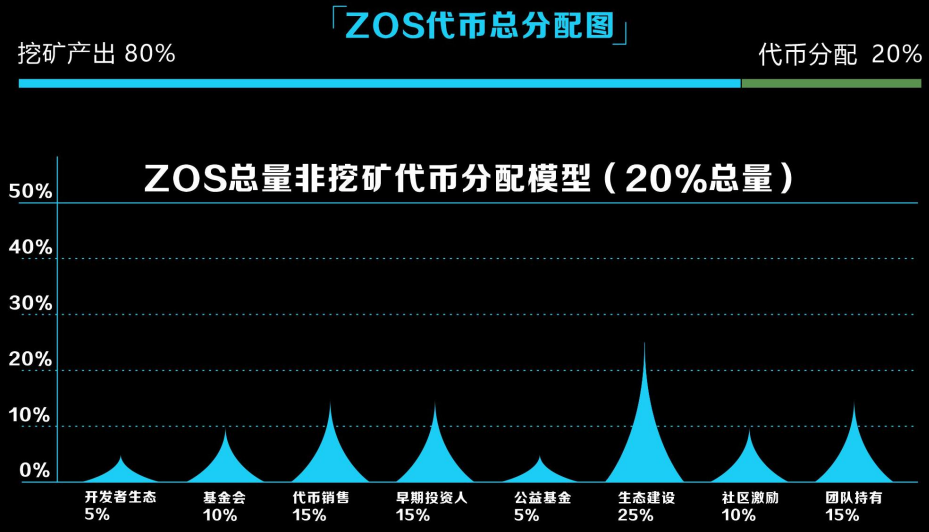
1.1 代币基本信息

ZOS公链采用原生统一基础货币体系 —— ZOS，主网未正式上线前，将发行基于以太坊的ERC20代币，总量10亿枚。

ZOS作为全球化元宇宙应用级基础公链Token，我们围绕它定制了一套完整的商业化生态落地体系，遵循安全透明、可靠、模块化、平行扩展等原则，提供与之对应的激励方案。ZOS作为本生态价值基础，通行于系统的所有环节，是一切费用与价值交换的标准价值单位。

1.2 ZOS代币分配

总量10亿



- 基金会10%　　锁仓三年，首年立即释放20%，第二年减半日释放30%，第三年减半日释放50%
- 早期投资者15%　　锁仓三年，首年立即释放20%，第二年减半日释放30%，第三年减半日释放50%
- 生态建设25%　　用于ZOS生态建设，奖励对ZOS生态做贡献的用户。
- 社区激励10%　　用于zos生态社区的发展激励
- 团队持有15%　　锁仓三年，首年立即释放20%，第二年减半日释放30%，第三年减半日释放50%

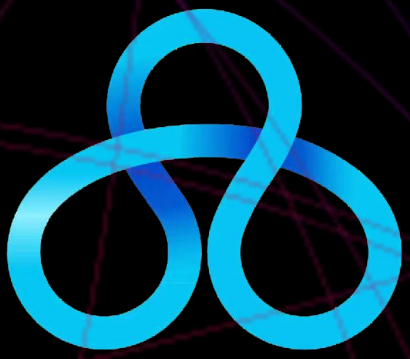
用途	占比	ZOS总量20%的代币分配具体说明
基金会	10%	ZOS基金会持有，用于团队整体规划与发展
创始团队	15%	ZOS团队持有，用于早期日常运营与激励
早期投资人	15%	ZOS早期投资人激励，鼓励早期生态建设者
公益基金	5%	ZOS公益基金激励，奖励对行业发展做出贡献的用户
生态建设	25%	用于ZOS生态建设，奖励对ZOS生态做贡献的用户
社区激励	10%	用于ZOS生态社区的发展激励
代币销售	15%	用于ZOS代币的早期销售
开发者生态	5%	用于ZOS技术团队的研发费用

1.3 代币挖矿产出与经济循环

ZOS生态80%的代币将由挖矿产出，首年产出两亿枚，挖矿锁仓机制为产出立即释放40%，剩余60%通过180天释放。减半时间约为苹果发布会的前一个月，每两年减半一次。

由于ZOS使用了ZPOS混合共识机制，官方将自建POW生态节点，这些节点将深度与各类技术机构合作，通过官方的专业智能挖矿设备来激活ZOS出块，提高网络性能，用户可以通过POS的方式，根据质押挖矿的行为获得ZOS代币产出。

在ZOS生态经济循环中的供给者，指的是促成主网顺利运行的工作者，他们要么通过计算能力较强的专业设备运行全节点挖矿软件，要么通过持有ZOS代币进行POS质押挖矿参与主网的治理，此后他们可以选择将ZOS拿至交易所贩售或保留，而贩售至交易所的ZOS未来又有机会被消费端需求者所购买，形成一个完整的经济循环。

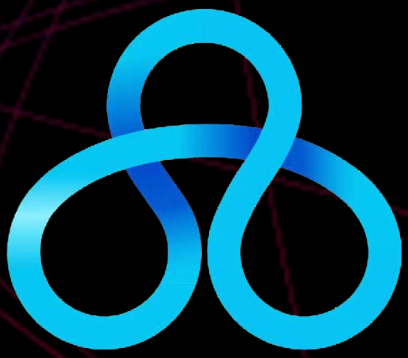


ZOS

未来规划路线

六、ZOS未来规划路线


2023.5
整体元宇宙商业生态成型，继续扩展元宇宙生态落地，加快周边产业部署实施
主网各类生态运行良好，社区激励与开发者生态日益完善
2023.1
2022.10
主网正式运行，元宇宙生态开始大范围落地，支持各类链游上链
主网研发成型，进入正式公测阶段，同时开启创世挖矿
2022.5
2021.10
核心技术完备，底层架构搭建完成，开始着手于测试与早期代币销售
根据当下行业公链技术困境，我们看到了机会，并决定开始打造ZOS应用级公链
2021.6



ZOS

团队成员

七、团队成员

1、团队概况

ZOS团队由来自硅谷各行多位专家组成，其核心创始成员在数学、区块链技术、计算机、金融、存储等领域均有十年以上从业经历。目前已经获得了SBCVC（软银）领投的350万美元种子轮融资，分布式资本、LD Capital、Brightway Future Capital、UpHonest Capital等机构参投。

2、成员介绍

1.1.1 首席执行官（Chief Executive Officer，CEO）

Sean Park 拥有超过 16 年的资本市场和投资银行高层工作经验，是金融服务未来的领先独立思想家、The Park Paradigm 的作者，曾经创立Anthemis Group。随着世界从工业时代进入信息时代，一个巨大的机会可以从金融服务和市场新范式的出现中获利。Sean的目标是建立一个全新的元宇宙底层系统，挑战传统金融，实现颠覆性的商业模式。

在担任ZOS首席执行官的同时，Sean 还是 Betfair、WeatherBill 和 BankSimple 等创新公司的创始投资者，并在过去十年中拥有丰富的

经验，为初创公司和高增长公司提供投资和咨询服务。

1.1.2 首席运营官 （Chief Operating Officer，COO）

Jeremy Johnson

Jeremy 与数字领域有前途的企业家合作，怀着帮助创造明天的全球领导者的谦逊雄心。具有遍布美国、欧洲和亚洲的全球经验和网络。作为一名商业和金融市场专业人士，Jeremy的职业生涯多种多样，从担任知名衍生品交易员和英国顶级银行的董事，到各个领域的创业企业。

对许多产品有深入而透彻的了解，并在商业业务的挑战中茁壮成长，对利润有敏锐的眼光，但有能力培养和发挥团队的最佳作用。

1.1.3 首席财务官（Chief Financial Officer，CFO）

Charlie Cox

Charlie 曾在金融行业的传统和数字领域工作。2017年，他开始了为期一年的 Digital Asset Management Ltd 实习，负责 OTC 交易（执行、保证金分析和报告）、营销（社交媒体广告、研究和分析）、数字资产交易流程、数字资产投资组合管理、业务发展（与直布罗陀

的主要利益相关者建立联系）和销售（冷电话和向潜在客户推销产品）。Charlie 于 2018 年 9 月在直布罗陀资产管理公司参加了为期两周的实习，涵盖资产管理的传统方面。这包括场外交易、投资组合管理、对冲和投资分析（股票、固定利率、商品、差价合约、期货和期权以及外汇）。在完成实习之前，他成功地参加了英国特许证券与投资学会 - 证券与投资概论。

1.1.4 首席信息官（Chief Information Officer，CIO）

Lance Morginn

Lance 是一位连续创业者，拥有 20 多年从头开始创建、领导和发展成功的数百万美元技术型企业的经验。他的背景包括担任少数上市公司和私营公司的创始人/首席执行官/董事. 2015 年，Lance共同创立了 BIG Blockchain Intelligence Group，现加入 ZOS 团队。

1.1.5 首席技术官（Chief Technology Officer，CTO）

Mike Ganbold 是一名技术高管，在前沿技术公司（从 Cambridge Analytica、ConsenSys 到 Intrepid Capital Partners、Fabric Ventures 和 Stelium Ventures）担任运营商的经验，并且擅长构建商业生态系统。他致力于通过与拥有相同愿景的一流技术创始人合作，建立有弹性、高效和公平的经济，曾就人工智能和区块链

技术的应用为全球企业和政府提供建议。通过与欧盟委员会、XPrize和联合国国际电信联盟的公开对话，Mike不仅帮助公司而且帮助公众了解什么是数据所有权，我们如何将自己的数据货币化以及围绕数据的道德规范。

1.1.6 首席营销官（Chief Marketing Officer，CMO）

Susana Esteban

Susana Esteban 毕业于剑桥大学MBA，将区块链等新技术与传统行业联系起来。 Susana 拥有丰富的管理经验，自 2005 年起在德国、西班牙、意大利和英国管理保险、服装行业以及房地产和资产管理团队。借贷、作为抵押品的 NFT、流动性池和抵押，以及在 50 多个国家和国际会议和小组中的演讲者。

基 金 会

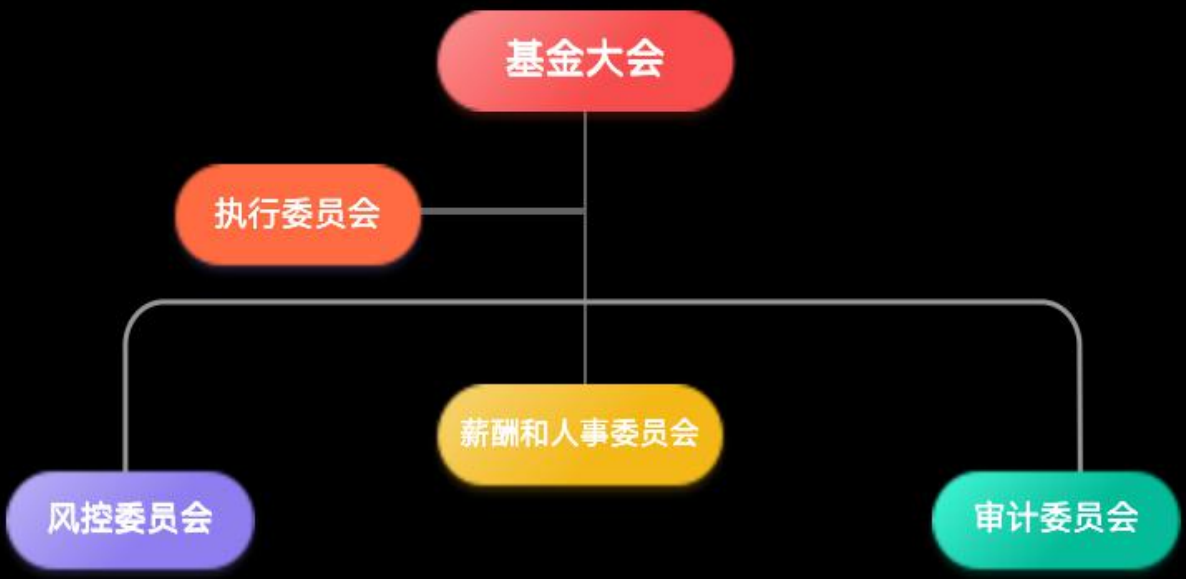
八、基金会

1、基金会概述

1.1 基金会简介

ZOS基金会（ZOS FOUNDATION LTD.）成立于新加坡，为符合当地法律法规设立的非盈利性公司。基金会致力于ZOS区块链底层技术、智能设备、元宇宙、链游生态建设等发展及研究，以及发行后督促团队成员根据路线图逐步实现全球商业生态落地。基金会将通过制定良好的治理结构，按照白皮书的要求帮助管理兑换的加密货币的使用情况。基金会组织架构主要由决策委员会、财务和市场及公共关系委员会组成。

1.2 基金会治理架构



1.3 各委员会职能划分

- 执行委员会

研究和拟定长期规划，制定章程和管理制度，新项目可行性分析研究及批准，管理日常运营。

- 风控委员会

研究和制定风险控制策略，制定风控标准，审核整体运营风险，召集项目风险审核会议并组织审核结果发布。

- 薪酬和人事委员会

拟定和修改薪酬、激励方案，审核机构设置及岗位设置，进行人员聘请。

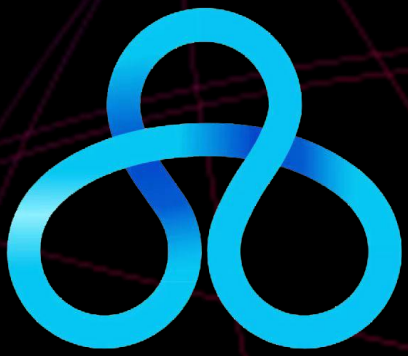
- 审计委员会

负责运营审计、财务审计、代码审计及 TOKEN 销毁等工作。

1.4 风险管控及法律事务

关于代币的发行、分配、智能合约代码（Smart Contract code）等代币发行的相关资料以及财务报告，基金会会挑选大型会记事务所，并实行每年一次的审计，把审计报告公布在网站上。

本白皮书的全部版权归属于基金会，未经基金会明确书面同意，任何个人或机构均不得私自修改、删减、复制、出版、印刷、传阅等等侵犯基金会合法版权的相关活动，基金会有权保留采用一切法律手段维护的权利。



风险提示及免责声明

九、风险提示及免责声明

➢ 风险提示

安全：许多数字资产因为安全性问题而停止运营。我们非常重视安全，但世界上不存在绝对意义上的 100% 安全，例如：由于不可抗力导致的各种损失。我们承诺尽一切可能确保您的资产安全。

竞争：我们知道区块链底层公链领域是一个竞争异常激烈的领域，有数百个团队正在计划并着手开发各种底层公链设施，竞争将是残酷的，但在这个时代，任何好的概念、创业公司、甚至是成熟的公司都会面临这种竞争的风险，但对我们来讲，这些竞争都是发展过程中的动力。

➢ 免责声明

该文档只用于传达信息之用途，并不构成买卖ZOS股份或证券的相关意见。

任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

ZOS基金会明确表示相关意向，用户明确了解ZOS的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。

ZOS明确表示不承担任何参与ZOS项目造成的直接或间接的损失，包括：

1. 因为用户交易操作带来的经济损失；
2. 由个人理解产生的任何错误、疏忽或者不准确信息；
3. 个人交易各类区块链资产带来的损失及由此导致的任何行为。

技术参考文献：

[1] Daniel Wang, Jay Zhou, Alex Wang, and Matthew Finestone. Loopring: A decentralized token exchange protocol.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.

[3] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151, 2014.

[4] Vitalik Buterin. Ethereum: a next generation smart contract and decentralized application platform (2013).

[5] Chris Dannen. Introducing Ethereum and Solidity. Springer, 2017.

[6] Jae Kwon and Ethan Buchman. Cosmos a network of distributed ledgers.

[7] Anonymous. aelf - a multi-chain parallel computing blockchain.

[8] Anton Churyumov. Byteball: A decentralized system for storage and transfer of value.

[9] Serguei Popov. The tangle.

[10] Colin LeMahieu. Raiblocks: A feeless distributed cryptocurrency network.